Tech Note 1055

Enabling OPC UA Discovery and Encryption

Topic#: t002900
Created: October 2014

Introduction

OPC UA Encryption allows for more secure, certificate-based, communications.

You can use OPC UA Discovery to allow you to browse for available OPC UA Servers, simplifying OPC UA Configuration.

Application Versions

- ArchestrA OPC UA Client Service v1.0

Assumptions

This *Tech Note* assumes you have already installed the following prerequisites:

- Application Server 2014 P01 or later
- ArchestrA OPC UA Client Service v1.0 or better
- Any 3rd party OPC UA Server
- We will use TOPServer 5.x and its simulation driver for this example

Prepare the System

1. In Windows Explorer, show hidden files and folders.

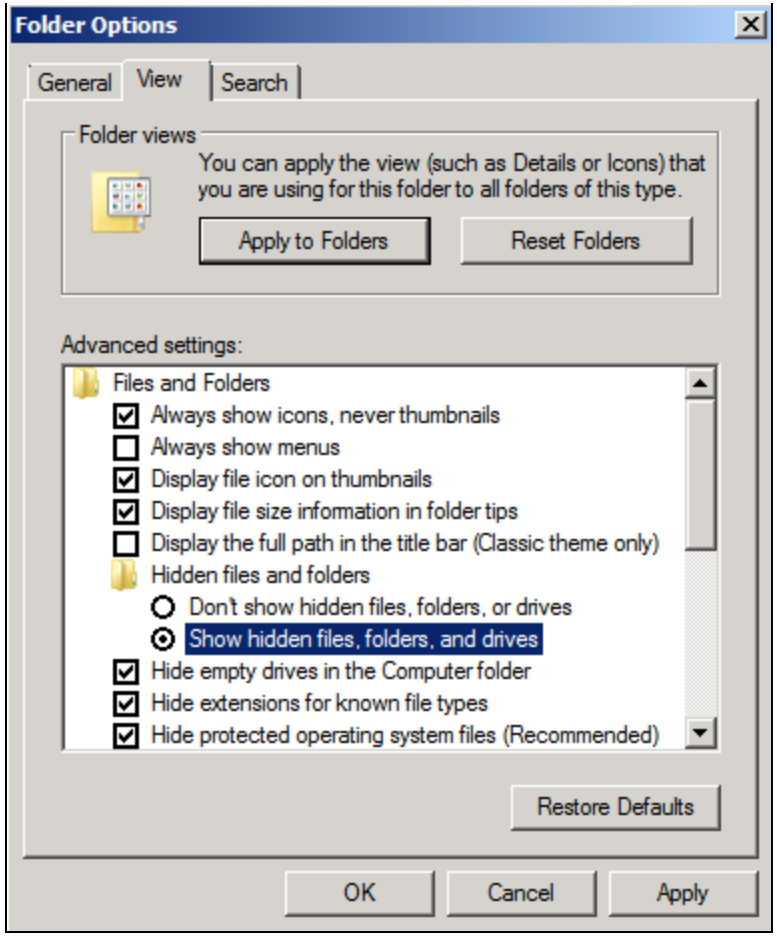

FIGURE 1: SHOW HIDDEN FOLDERS

2. Download and install OPC UA SDK Sample Applications v1.02 from the OPC Foundation (http://www.opcfoundation.org). It is located under Developer Tools - Developer Kits - Unified Architecture - Sample Applications:
   Direct link: https://opcfoundation.org/developer-tools/developer-kits-unified-architecture/sample-applications.

Create an ASB OPCUA Client Service Instance

Create an ASB OPCUA Client Service instance in the IDE (this generates the required client certificate).

1. Click **Galaxy>Configure>ArchestrA Services**.

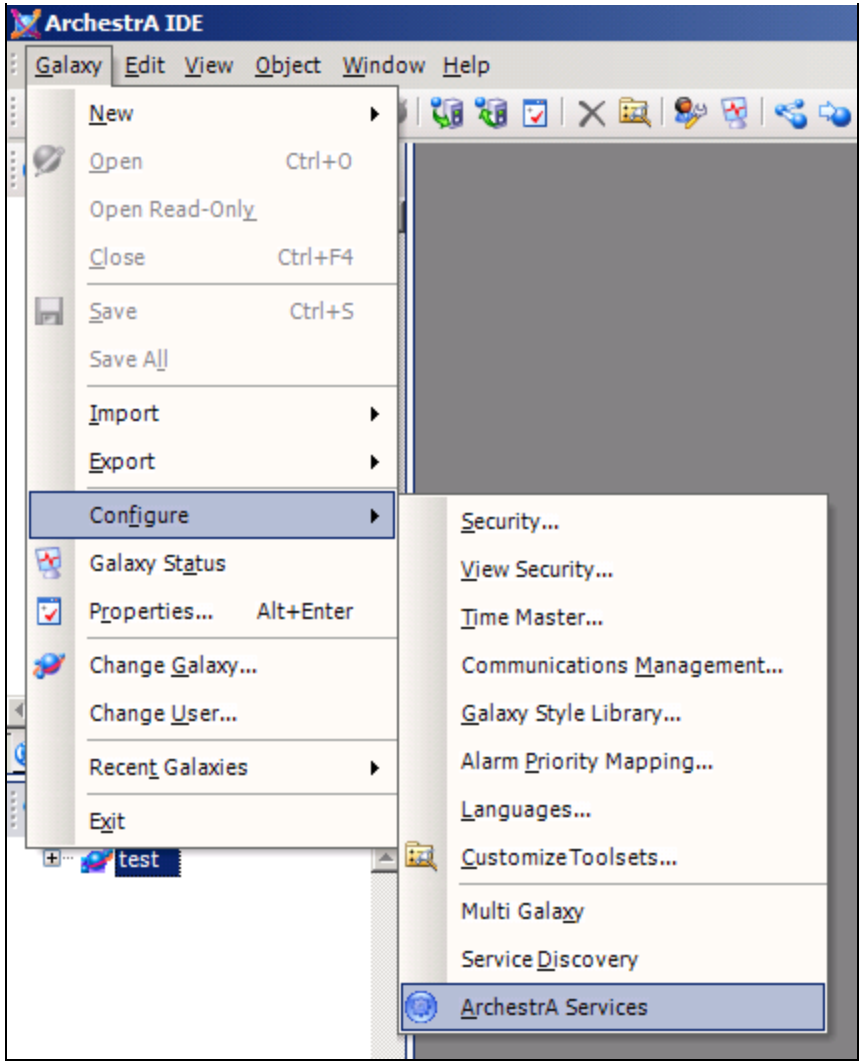

FIGURE 2: CONFIGURING ARCHESTRA SERVICES

2. Right-click **ASBOPCUAClientService** and choose **Create**.

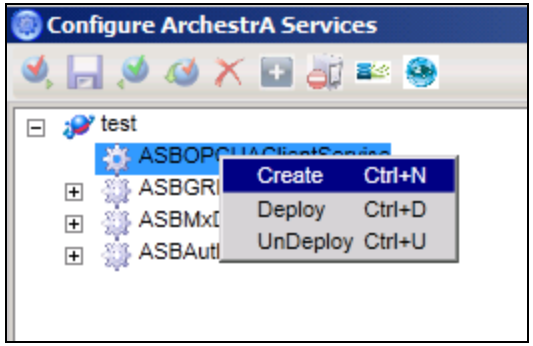

Figure 3: Creating an ASB OPC UA Client Service Instance

Configure OPC UA Server Security Settings

1. From the Start menu, click **Start>All Programs>Software ToolBox>Top Server5>OPC UA Configuration**.
2. Click on **Server Endpoints** tab.
3. Enable or create a Server endpoint that uses the computer node name.
4. Set your desired encryption method (Basic256, Sign & Encrypt in this case).

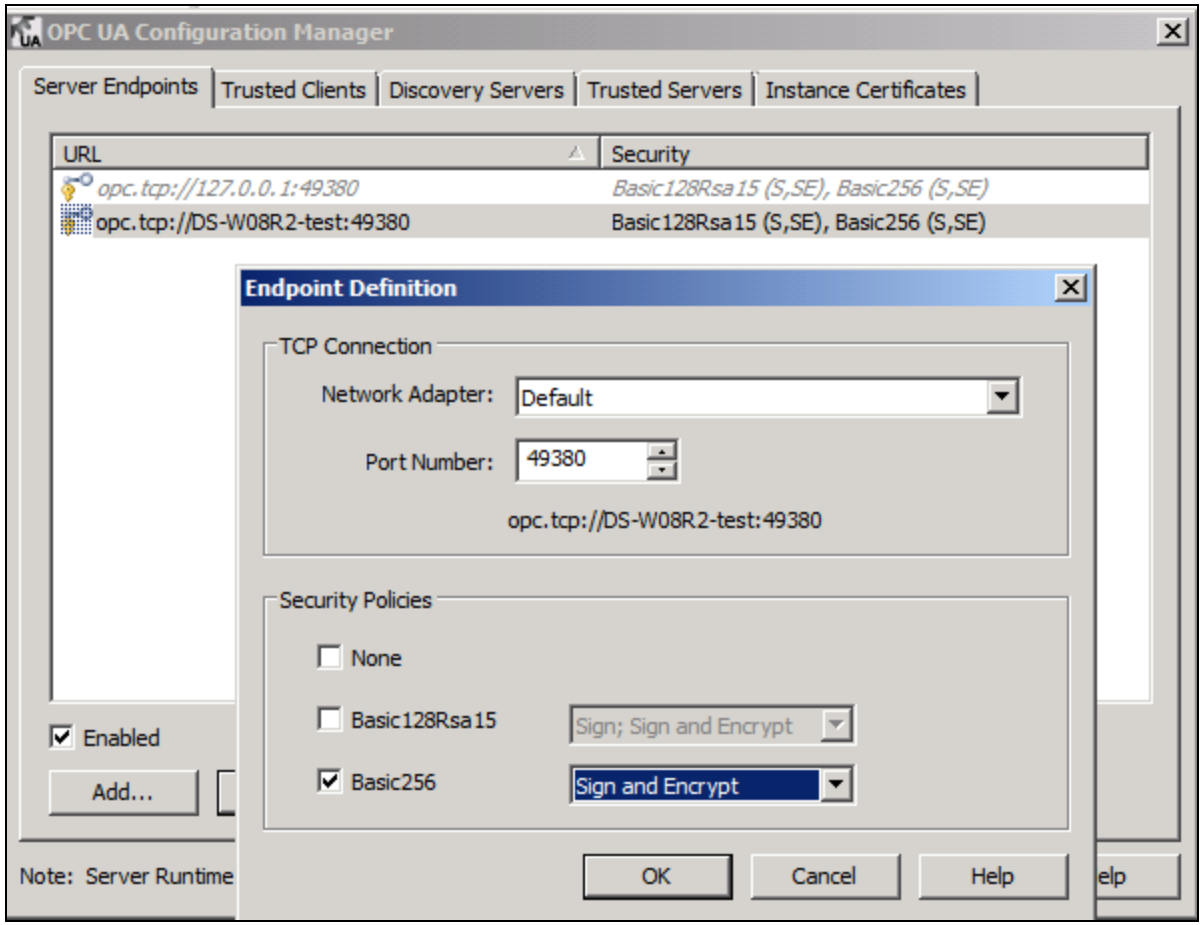

Figure 4: Choose Server-side Encryption

5. Click the **Trusted Clients** tab and import the ArchestrA OPC UA Client Service Certificate from: C:\ProgramData\ArchestrA\CertificateStores\OPCUAClient\certs\aaUAClient.def.

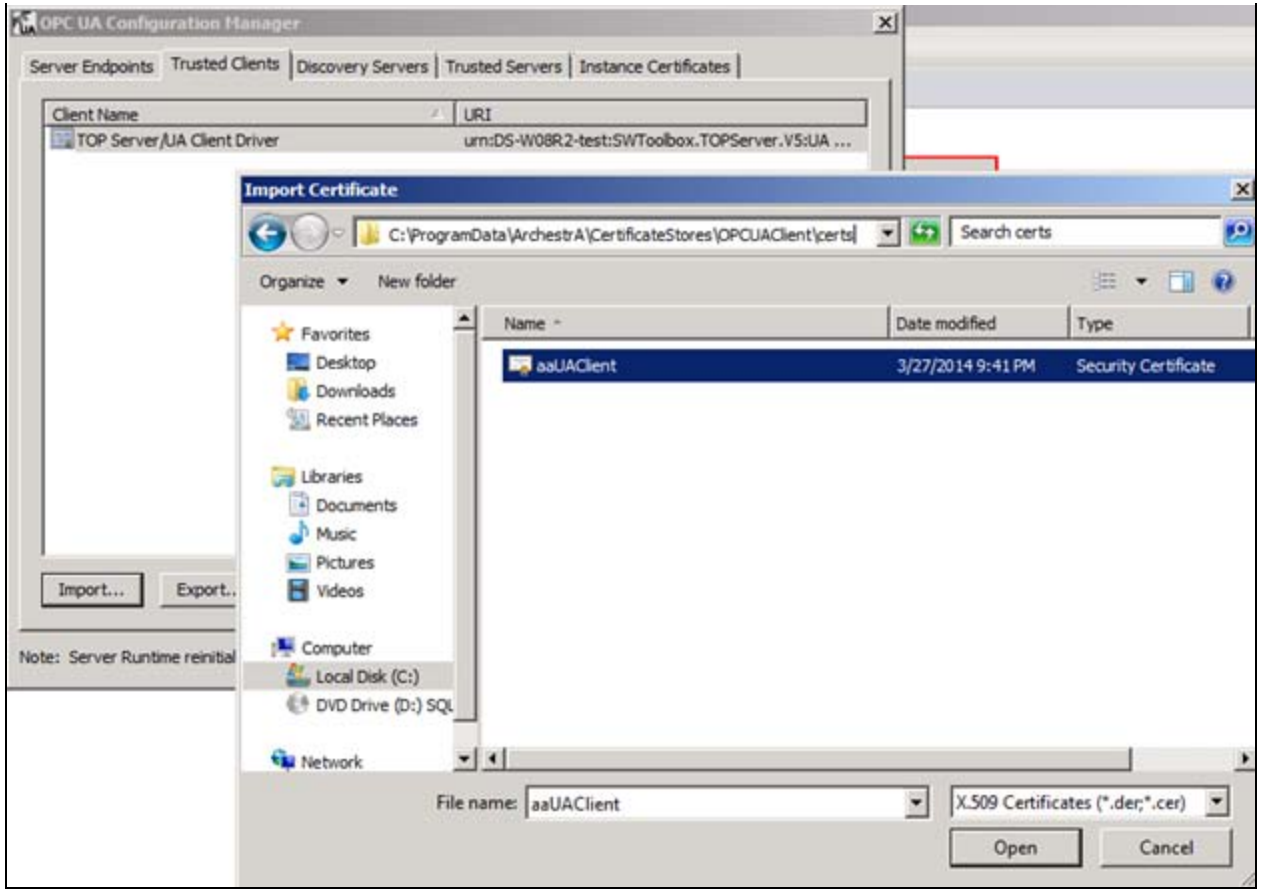

Figure 5: Define Trusted Clients

6. Click the **Discovery Server** tab.
7. Import the Discovery Server certs from: C:\Program Data\OPC Foundation\UA\Discovery\pki\own\ualdscert.der.

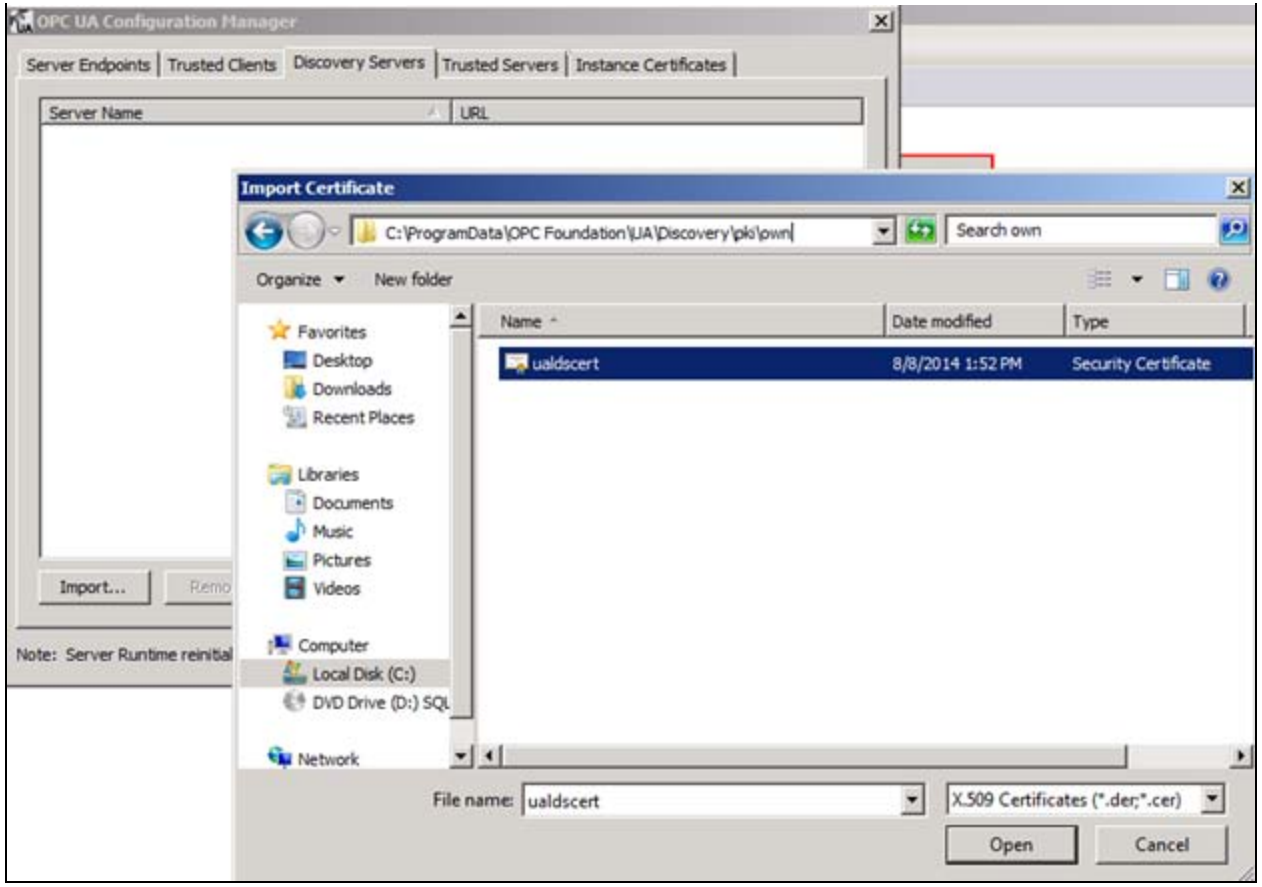

FIGURE 6: LINK OPC UA SERVER TO DISCOVERY SERVER

8. Click the **Instance Certificate**s tab.
9. Export the Server Certificate to a temporary location like Documents and give it a name with a '.der' extension

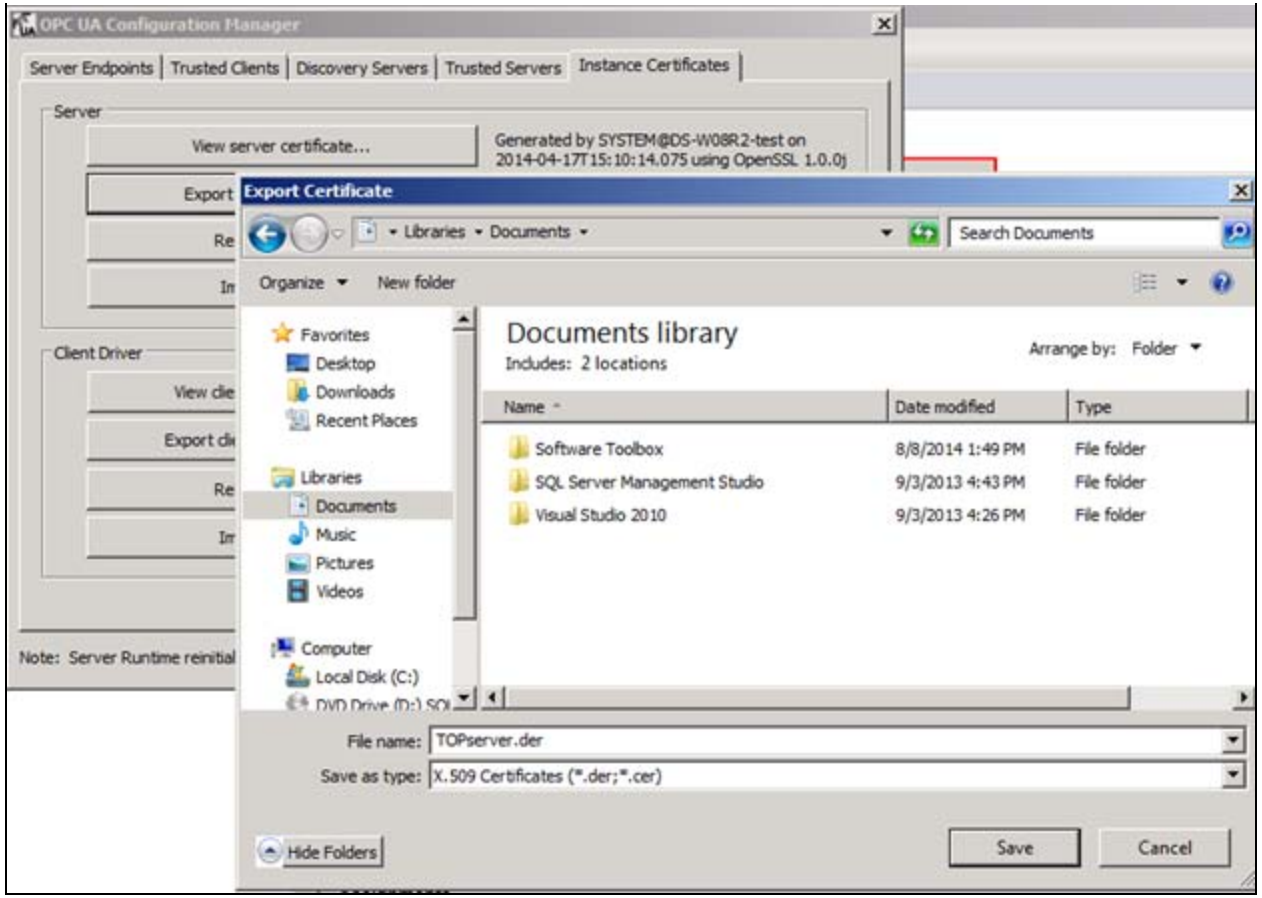

FIGURE 7: EXPORT SERVER CERTIFICATE

10. Close the OPC UA Configuration Manager.
11. Reinitialize TOPServer Runtime for changes to take effect.

Configure OPC UA Discovery Security

1. Open the OPC Foundation OPC UA Configuration Tool (Start>All Programs>OPC Foundation>Unified Architecture>1.02>Sample Applications>Configuration Tool).
2. Click the **Manage Certificates** tab.
3. Select the **Directory Store %CommonApplicationData%\OPC Foundation\CertificateStores\MachineDefault** Store Path.

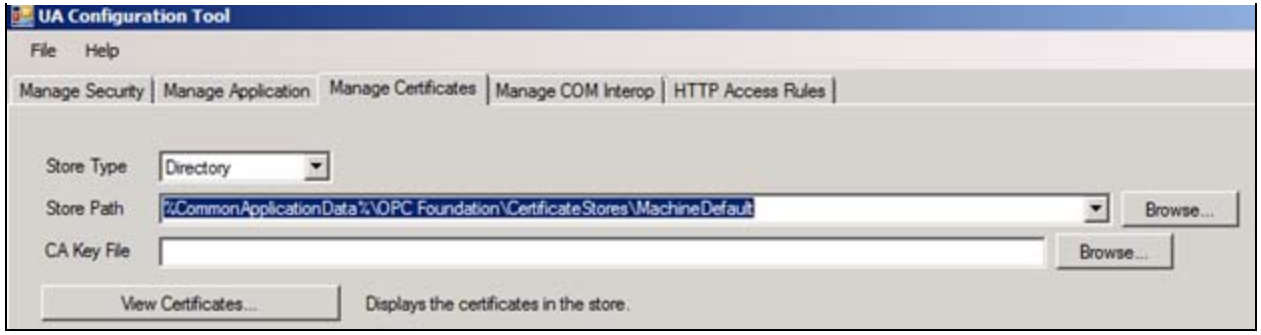

FIGURE 8: CHOOSE CERTIFICATE STORE

4. Press the **Import Certificate to Store** button.
5. Browse to **C:\Program Data\OPC Foundation\UA\Discovery\pki\own\ualdscert.der**, and click Open to confirm.

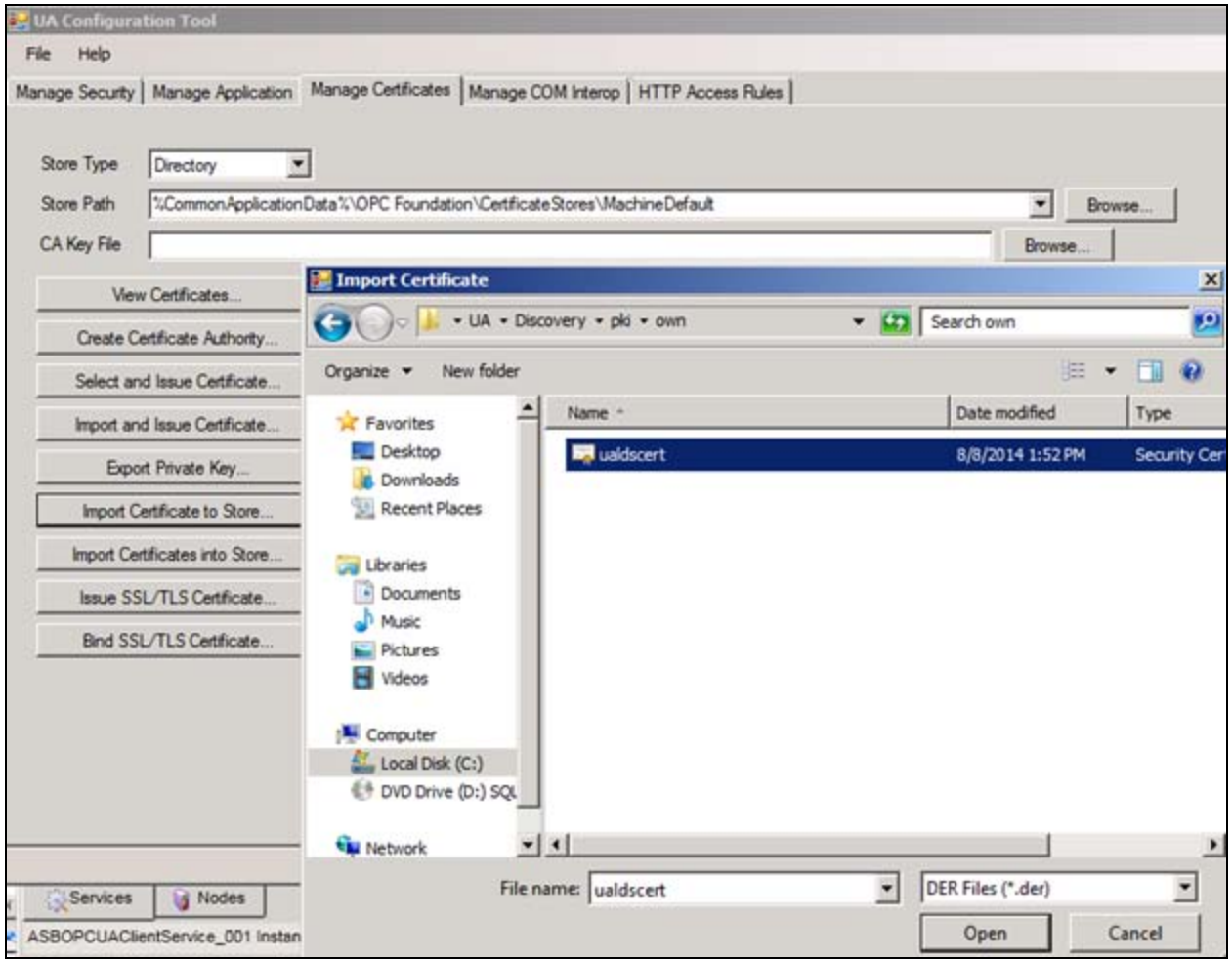

FIGURE 9: IMPORT DISCOVERY SERVER CERTIFICATE

6. Click **Yes** to accept the Certificate.

Figure 10: Accept the Certificate

7. In the OPC Foundation OPC UA Configuration Manager, click the Manage Security tab.
8. Choose Application to Manage OPC.UA.DiscoveryServer and press Edit.

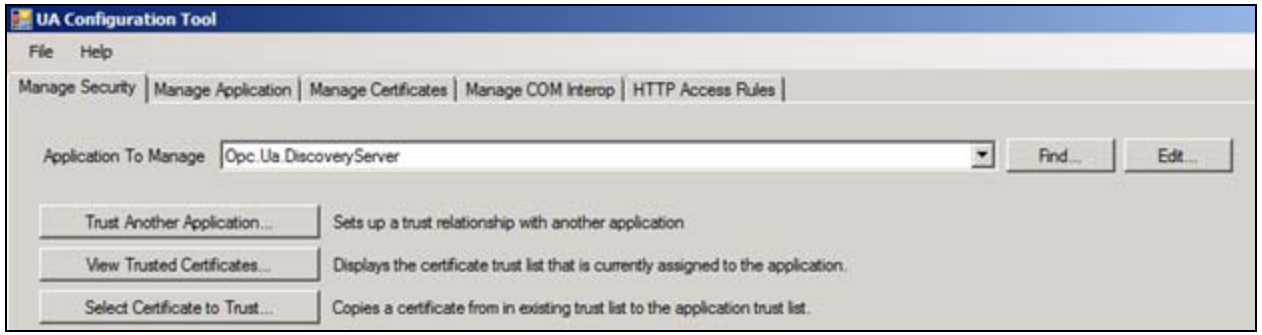

Figure 11: Setup Discovery Server Security

9. On the Certificate line, press Browse.

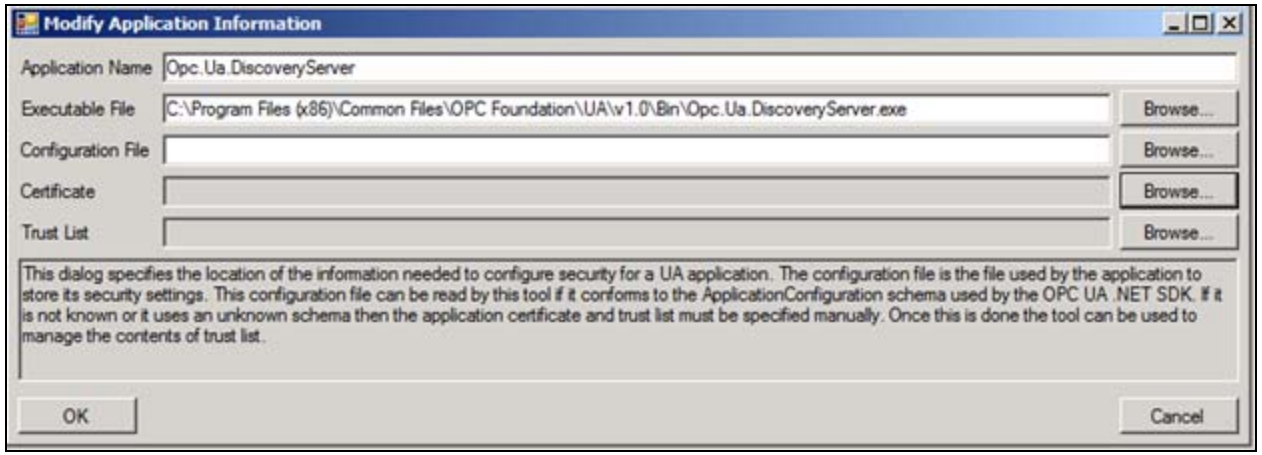

Figure 12: Modifying Discovery Server Application

10. Choose the Directory Store Type and MachineDefault Store.

11. Select the UA Local Discovery Server certificate, and click OK.

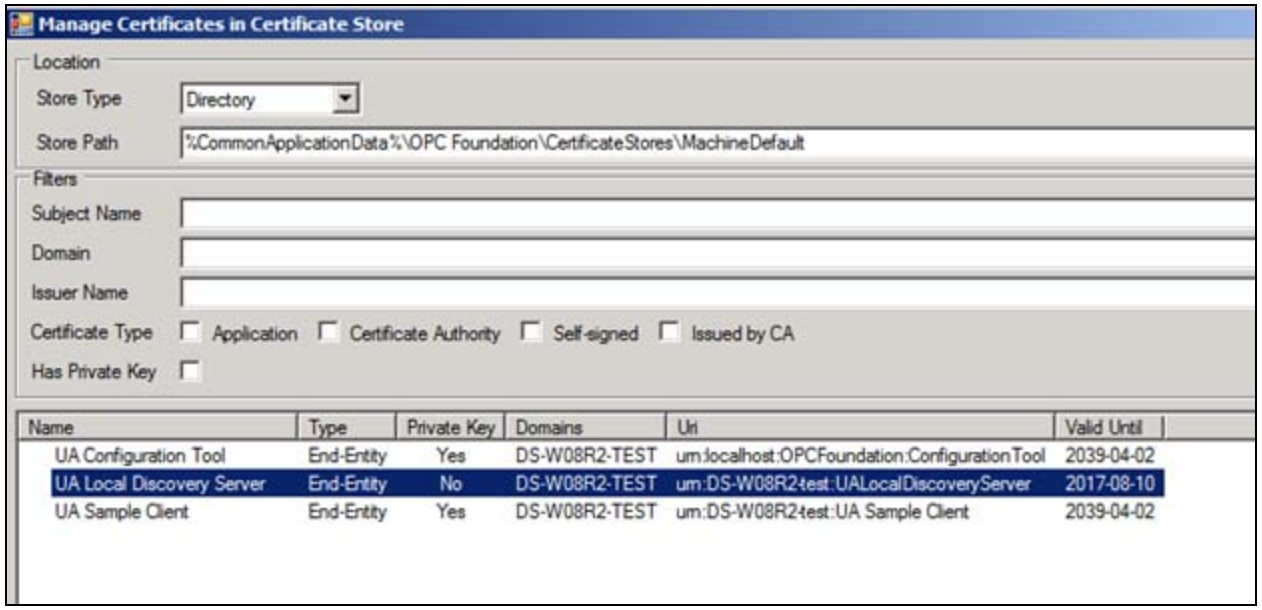

FIGURE 13: CHOOSE DISCOVERY SERVER CERTIFICATE

12. On the **Trust List** line, press **Browse**.

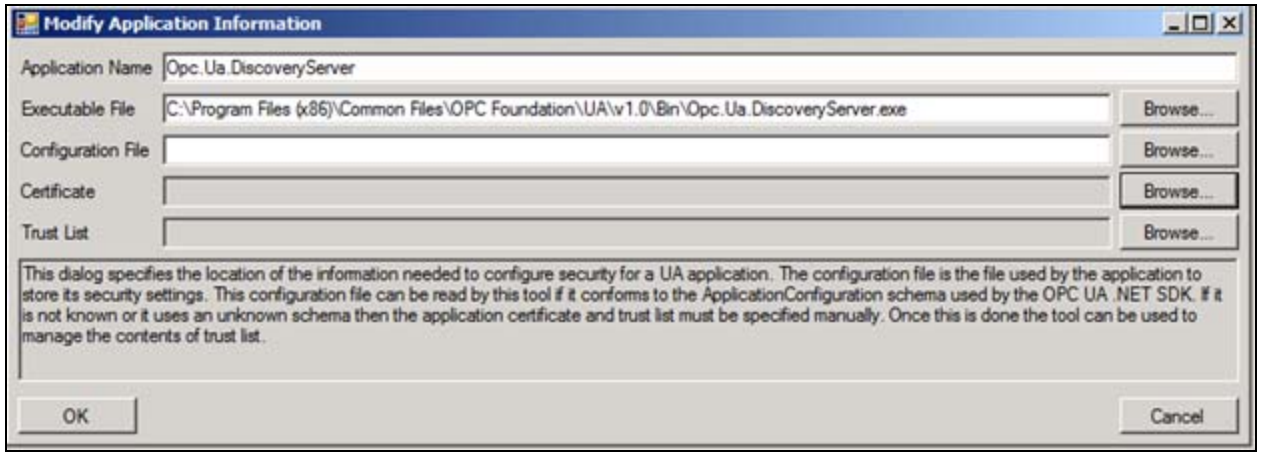

FIGURE 14: MODIFYING DISCOVERY SERVER APPLICATION

13. Select **Windows** Store Type, and path **LocalMachine\UA Applications**, then click **OK**.

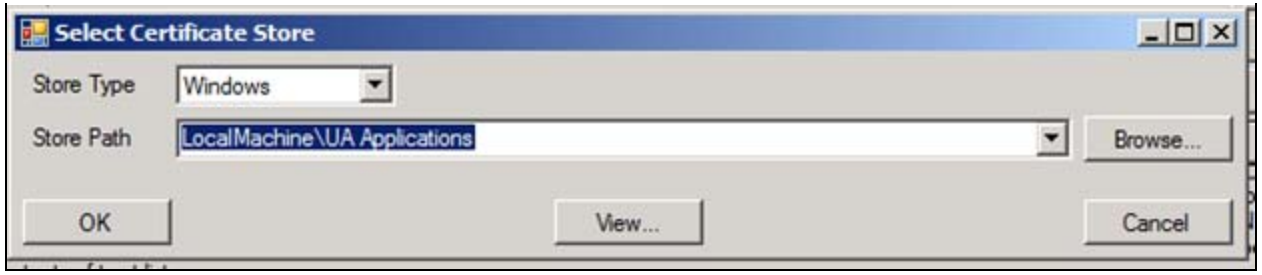

Figure 15: Choose Windows Certificate Store

14. Click **OK** to confirm your Application changes and click **Yes** to Overwrite.

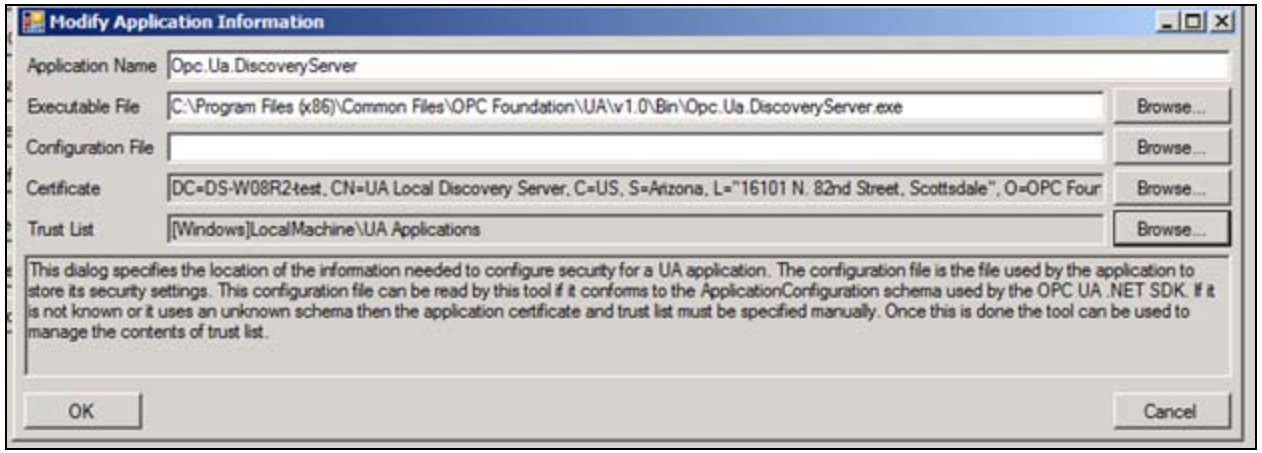

Figure 16: Save Discovery Server Application Changes

15. Click the **Manage Certificate** tab and click the **Windows** Store Type and the path **LocalMachine\UA Applications**.

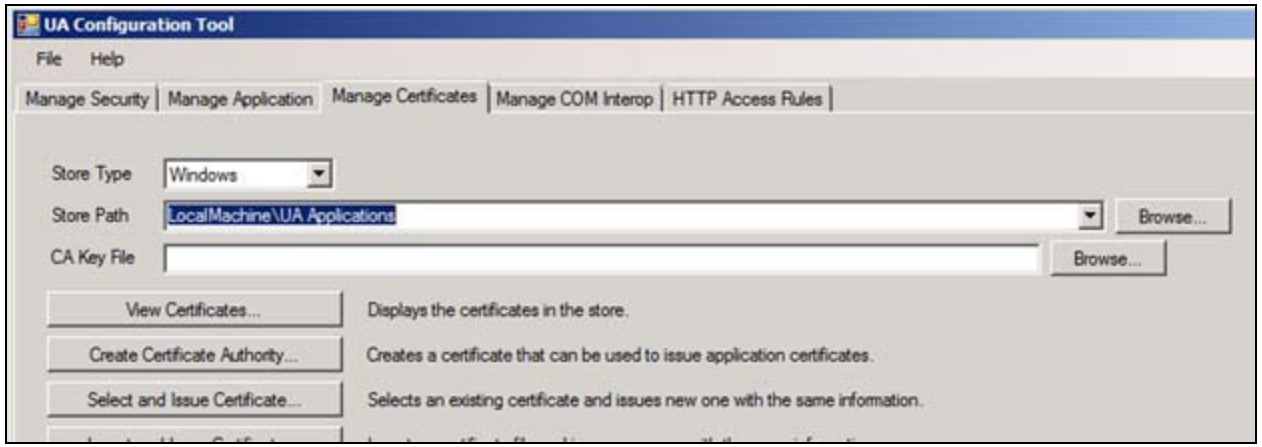

Figure 17: Manage Windows Certificate Store Certificates

16. Select **Import Certificate to Store**.

17. Browse to the **Top Server** certificate that you exported earlier to My Documents and click **Open**.

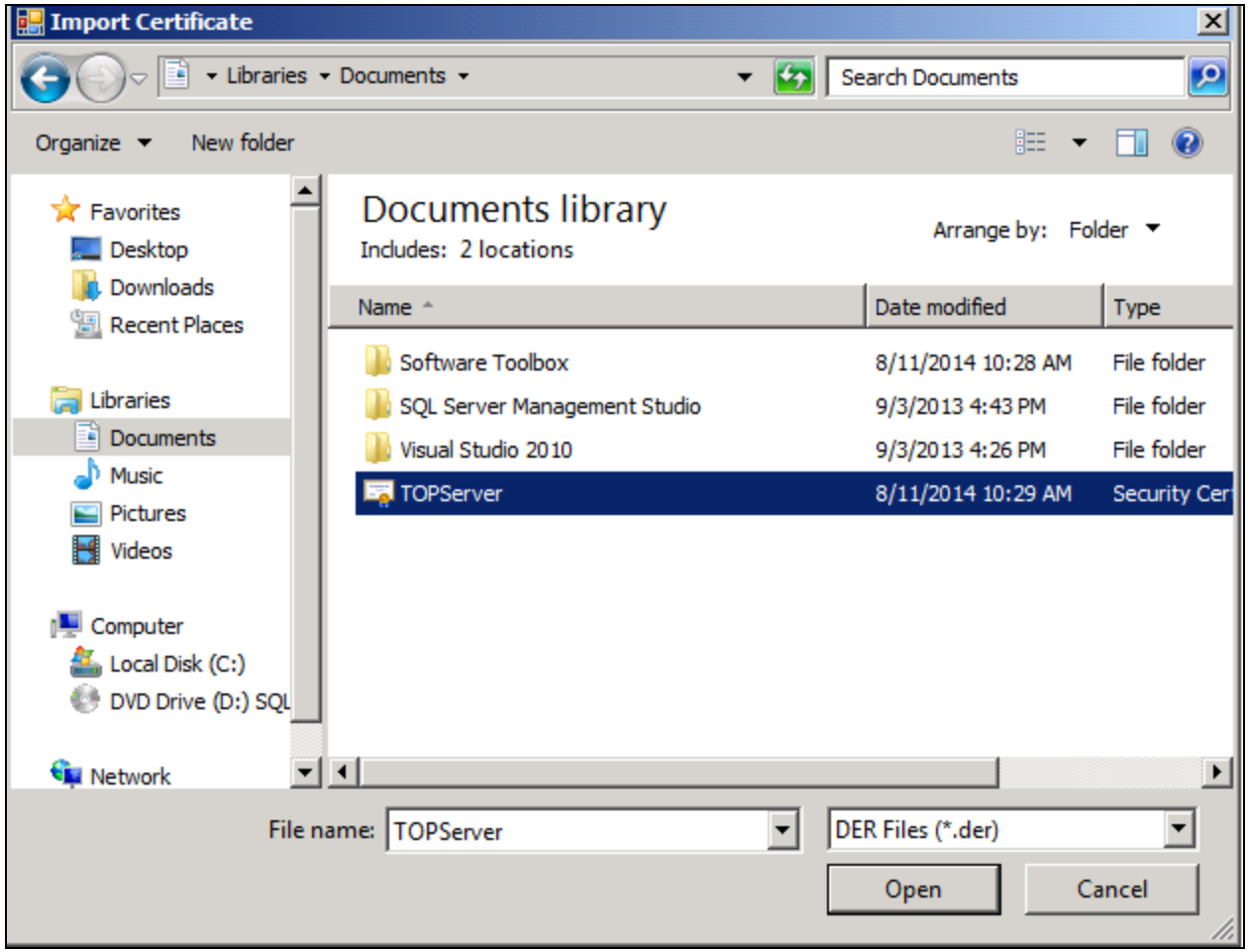

Figure 18: Import OPC UA Server Certificate to the Windows Certificate Store

18. Click **Yes** to accept the Import.

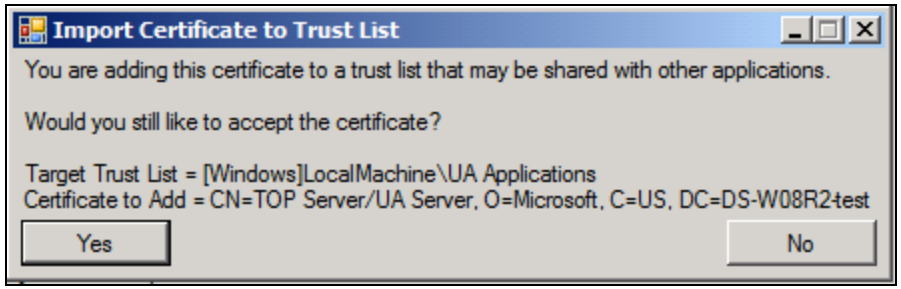

Figure 19: Confirm Certificate Import

19. Click the **Manage Security** tab and with **OPC.UA.DiscoveryServer** selected, click **Select Certificate to Trust**.

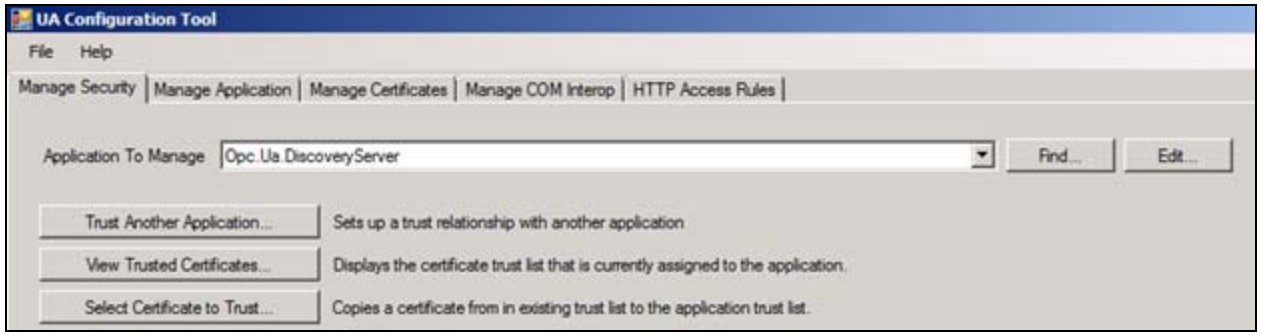

FIGURE 20: EDIT DISCOVERY SERVER SECURITY

20. Select the **Windows** Store Type and the path **LocalMachine\UA Applications**, then select the TOPServer certificate and click **OK**.

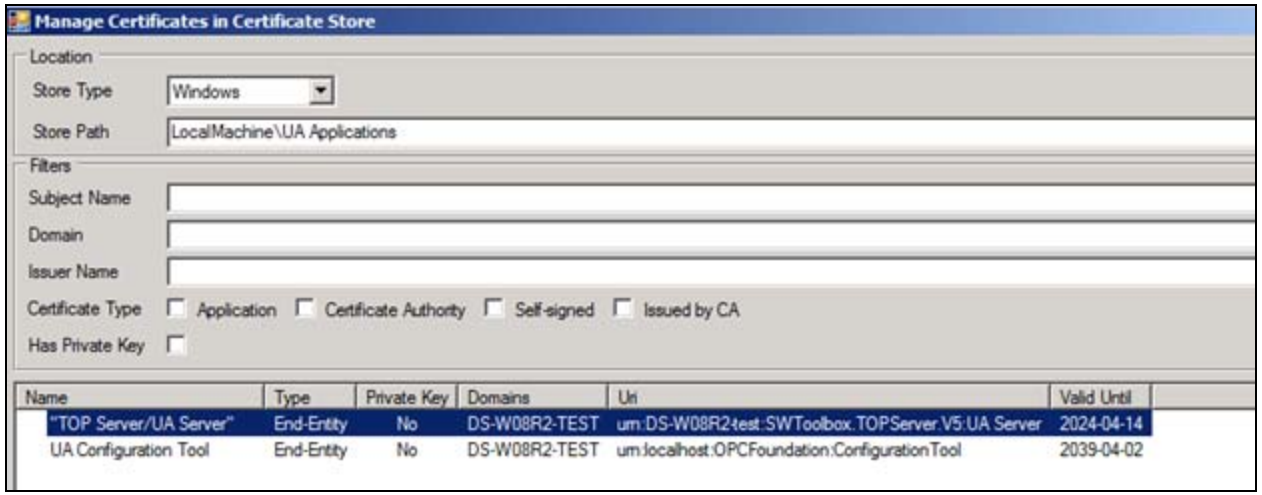

FIGURE 21: SELECT SERVER CERTIFICATE TO TRUST

21. Click **OK** to acknowledge the Trust.

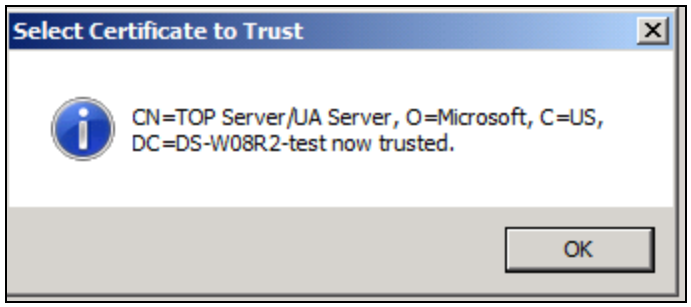

FIGURE 22: CONFIRM TRUST RELATIONSHIP

Configure the OPC UA Client Instance

1. In the IDE, right-click and check-out the **ASB OPC UA Client Service** instance.

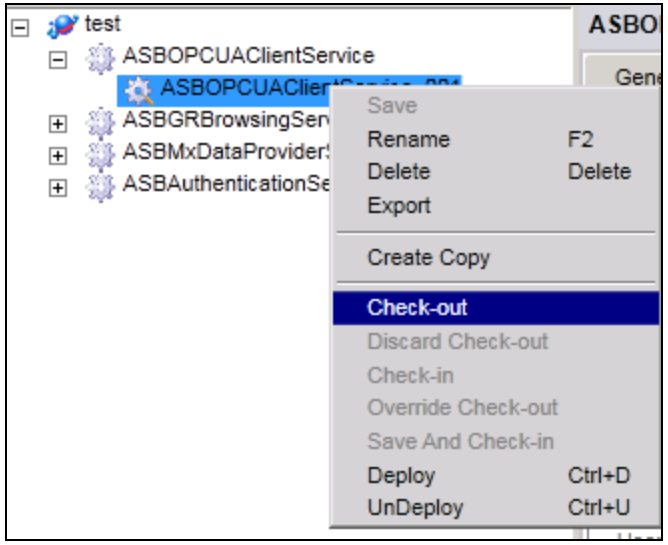

FIGURE 23: CHECK-OUT ASB OPC UA CLIENT SERVICE INSTANCE

2. Give it a Scope Name of your choice.

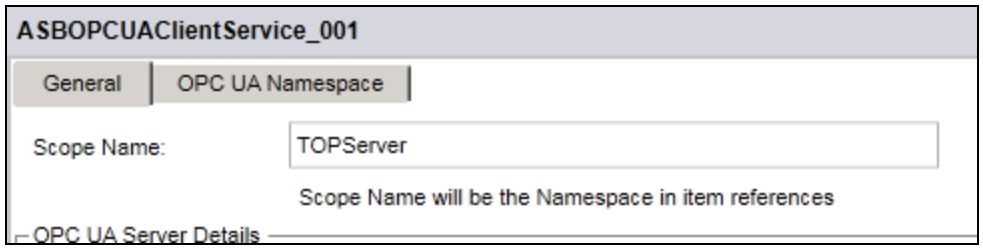

FIGURE 24: PROVIDE SCOPE NAME

3. Provide or browse for the OPC UA Server Node name.

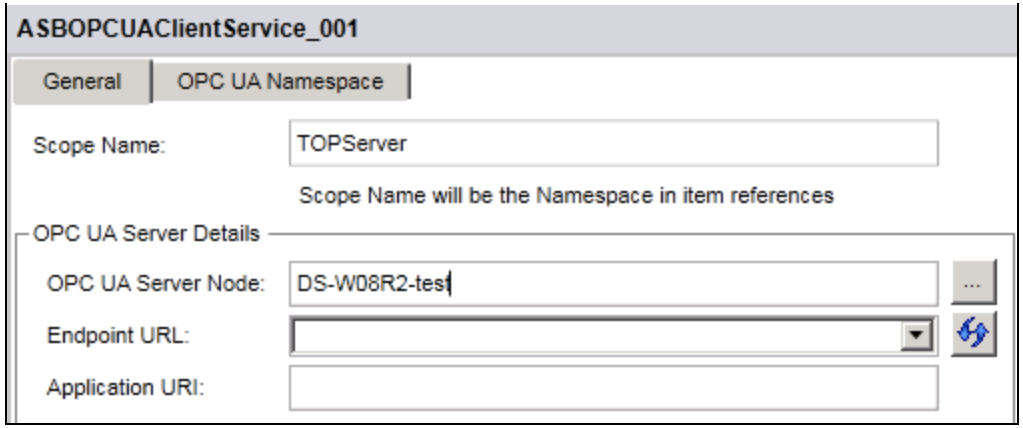

FIGURE 25: DEFINE OPC UA SERVER NODE

The Endpoint URL list populates when you press the drop-down and select your Endpoint URL.

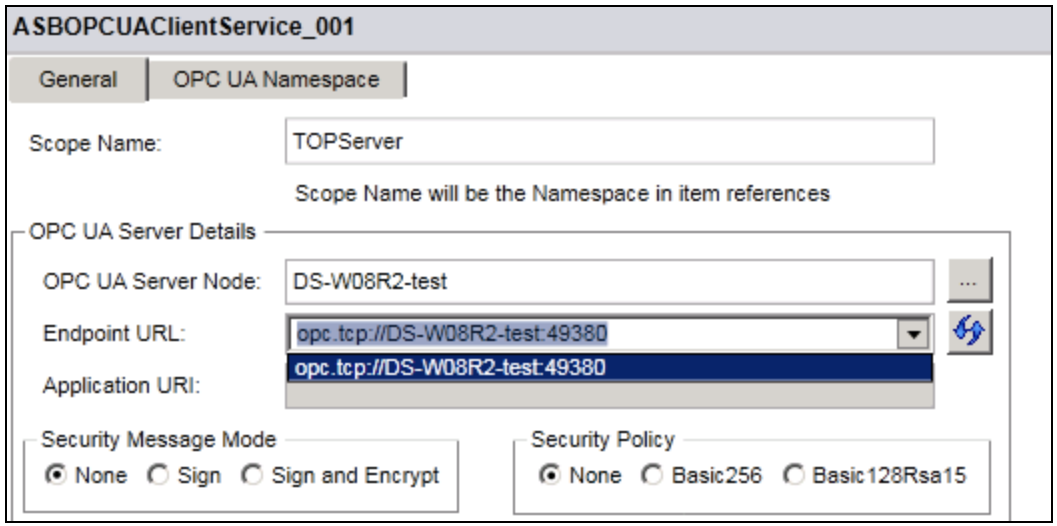

FIGURE 26: CHOOSE OPC UA ENDPOINT URL

4. Set your Encryption to match the server.

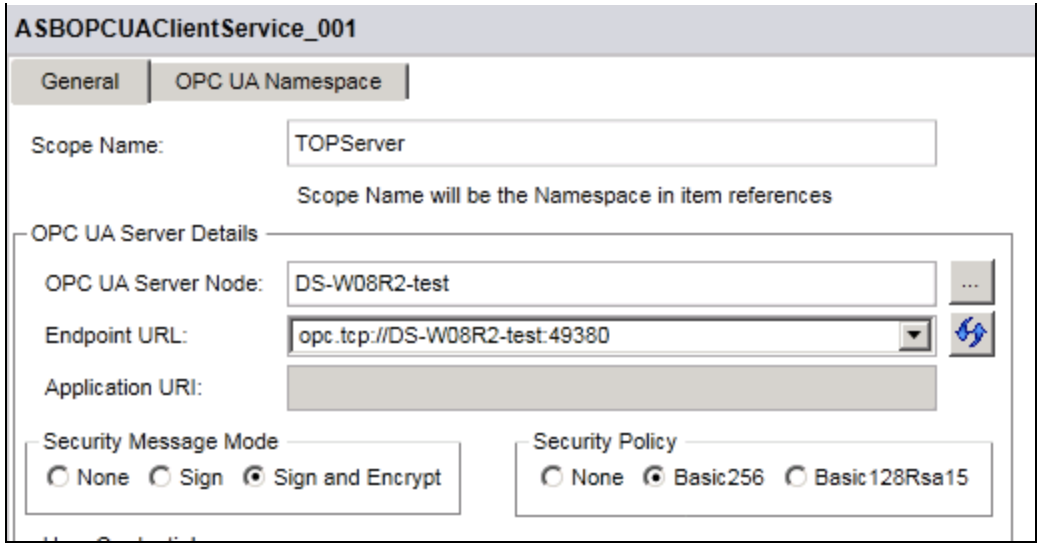

FIGURE 27: MATCH ENCYPTION TO SERVER-SIDE SECURITY

5. Go to the OPC UA Namespace tab to make sure it populates

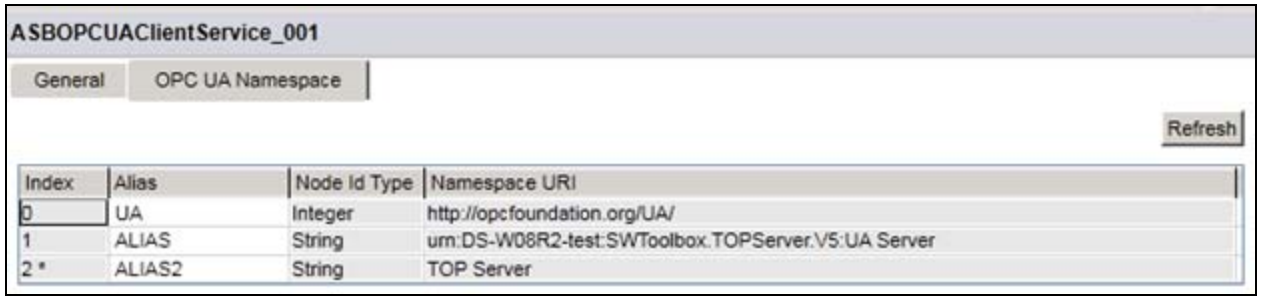

FIGURE 28: VERIFY NAMESPACE BROWSING

6. Click the **General** tab and assign the platform where this will be deployed, then press **Update**.

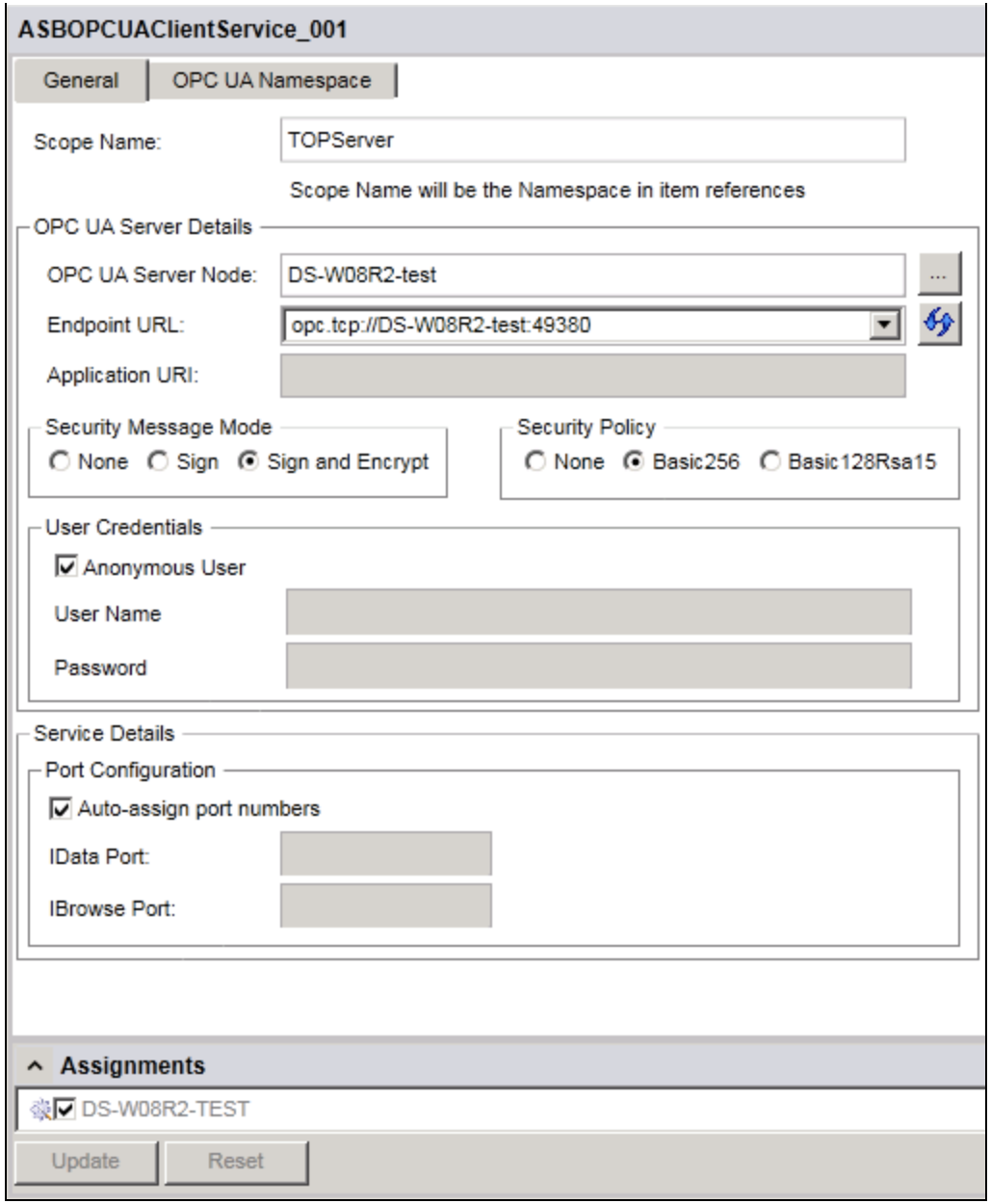

FIGURE 29: CHOOSE WHERE OPC UA CLIENT SERVICE WILL BE INSTALLED

7. Save, check-in, and deploy the ASB OPC UA Client Service Instance.

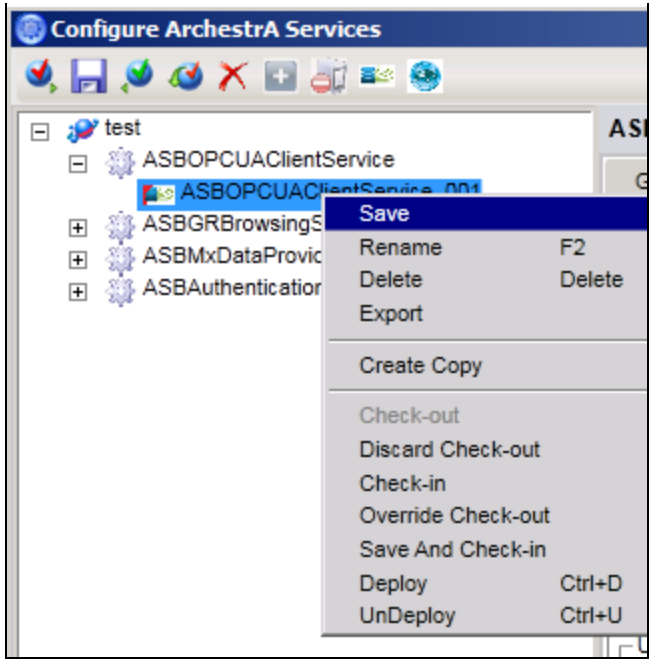

FIGURE 30: SAVE CHANGES

Create a User Defined Object Instance

1. In the IDE, create a User Defined Object (UDO) instance. this Object will be used to read IO data from the OPC server.

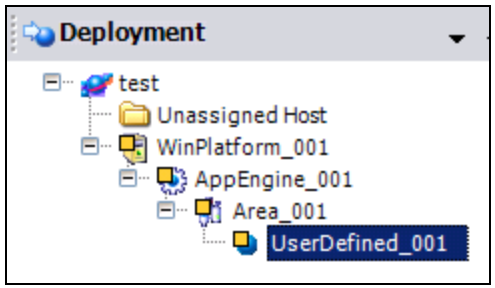

FIGURE 31: CREATE A UDO TO READ OPC UA IO DATA

2. Create a field attribute.

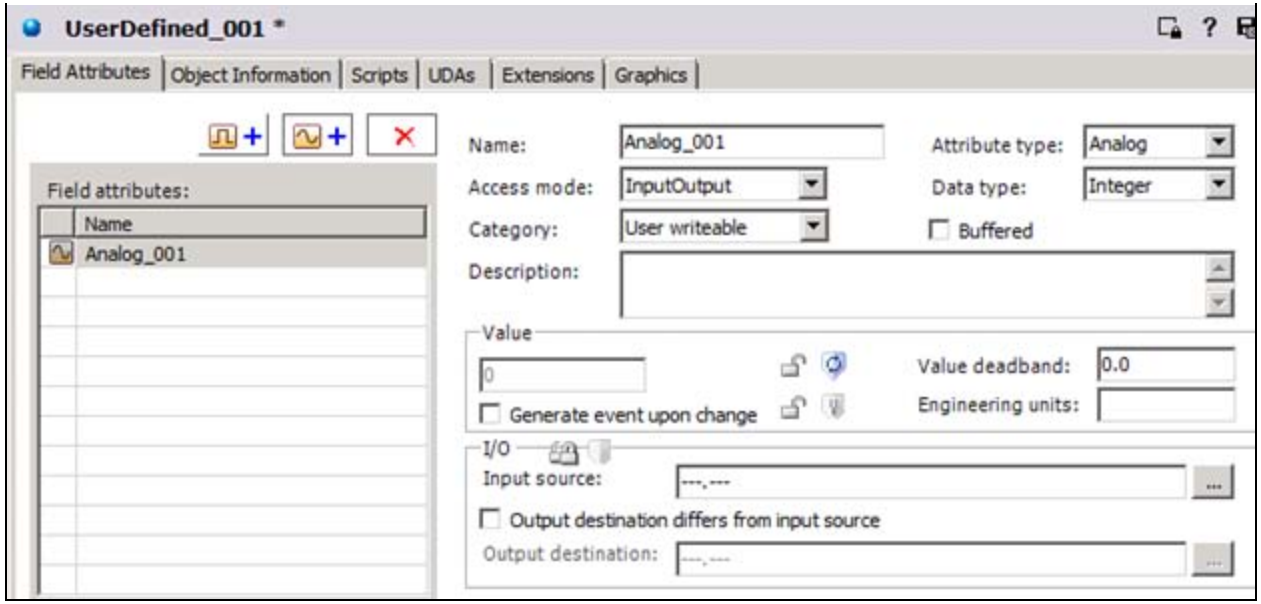

Figure 32: Define a Field Attribute

3. Click the **Attribute Browser** button next to the **Input Source** field.

4. Choose the Namespace that correlates to your ASB OPC UA Client Service instance and the left panel will populate with the server namespace.

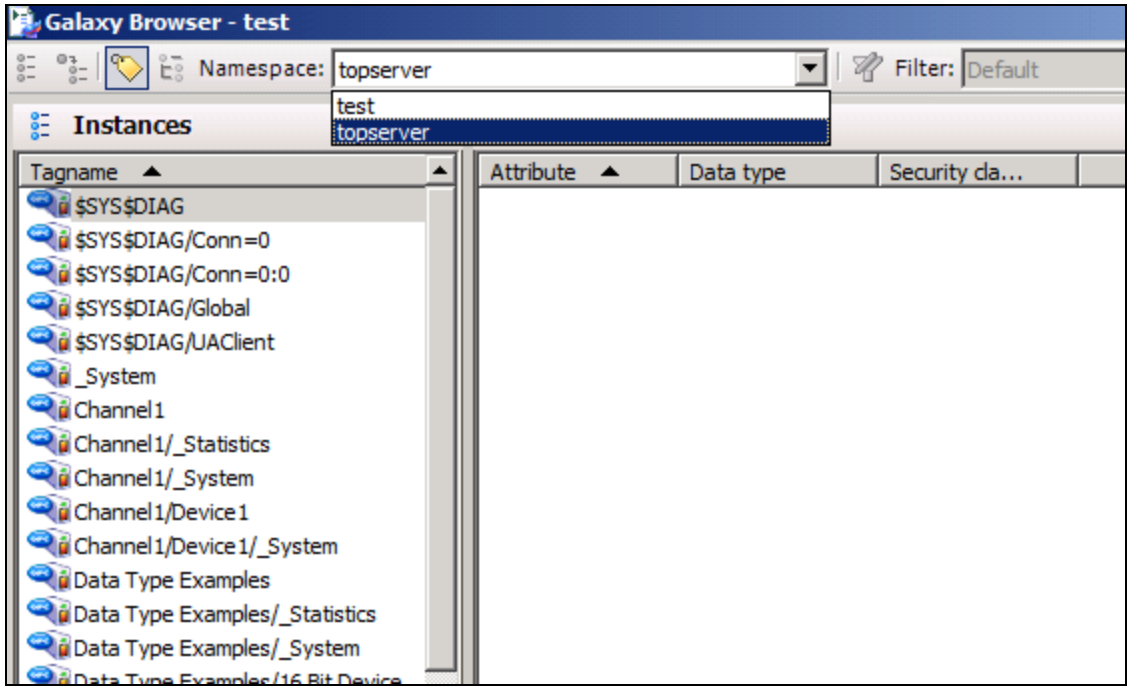

Figure 33: Choose the ASB OPC UA Client Service Instance Scope Name

5. Browse the OPC UA Server namespace and select a tag. Click **OK**.

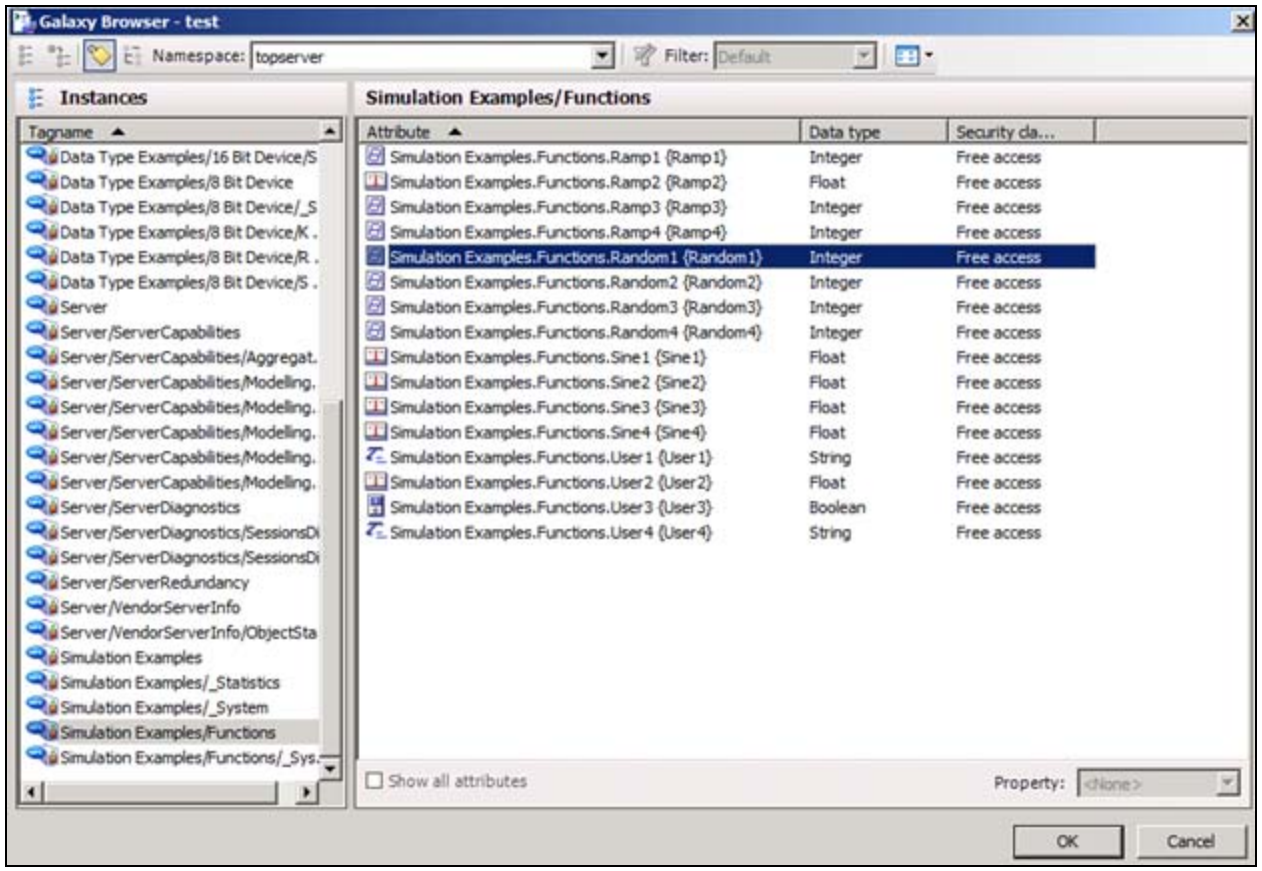

FIGURE 34: BROWSE THE OPC UA SERVER NAMESPACE

6. Save and Deploy the object. You can now view the tag in Object Viewer.

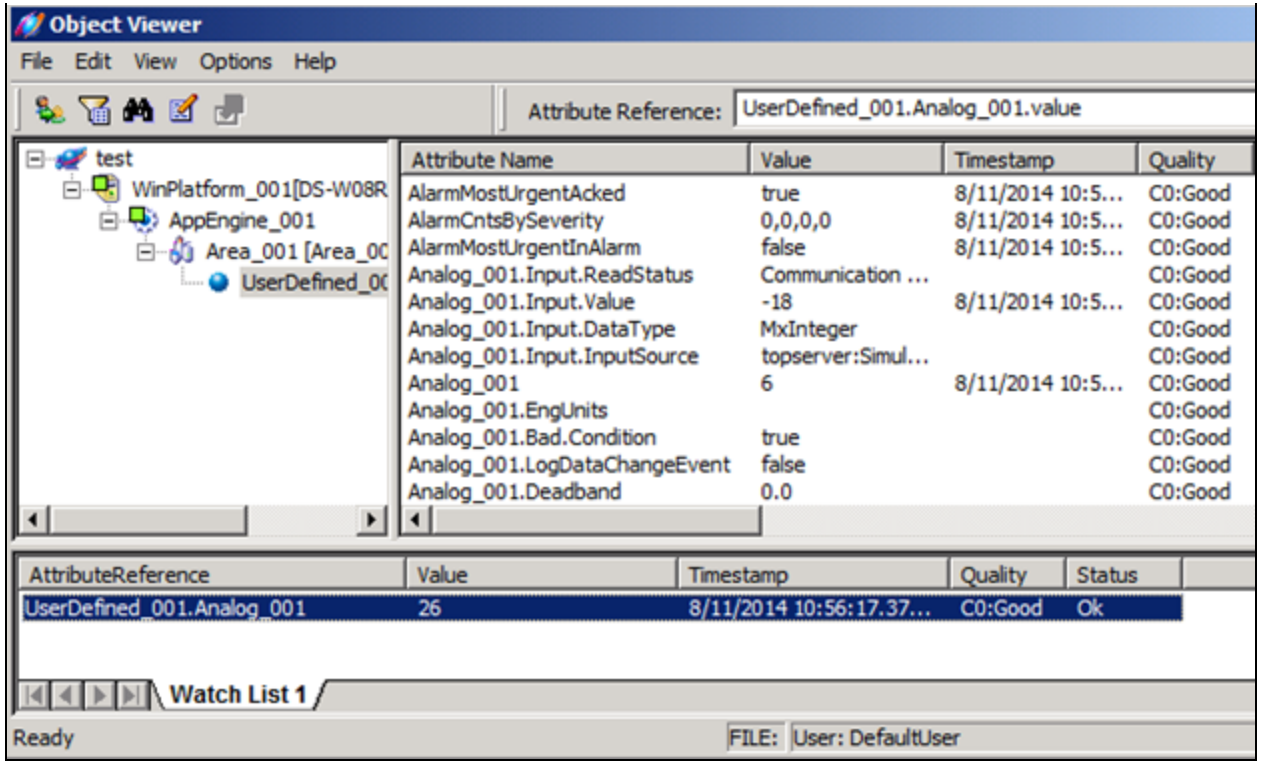

Figure 35: Deploy and View IO Data

D. Scott and G. Alldredge

Tech Notes are published occasionally by Wonderware Technical Support. Publisher: Invensys Systems, Inc., 26561 Rancho Parkway South, Lake Forest, CA 92630. There is also technical information on our software products at **Wonderware Technical Support.**

For technical support questions, send an e-mail to **wwsupport@invensys.com**.

Back to top